

CLAIMS - MARK-UP COPY

RECEIVED
CENTRAL FAX CENTER

SEP 08 2006

1. (Currently Amended) A computer-implemented method for securely transmitting an information package from a sender to an addressee via a network, the method comprising the steps of:

~~determining~~ searching at least one database to determine whether the addressee has a public key in order to determine the type of encryption to be performed on the package;

~~in response to~~ upon a determination that the addressee not having a public key;

does have a public key, encrypting the package with the addressee's public key and not encrypting the package with an escrow encryption key;

key;

only upon a determination that the addressee does not have a public key, selectively encrypting the package with the escrow encryption key;

storing the escrow key encrypted package in escrow for the addressee prior to receiving a public key for the addressee;

notifying the addressee of the package stored in escrow; and

in response to receiving an acknowledgement from the addressee:

issuing new public and private keys to the addressee, where said new public key is not equal to said escrow encryption key; and

in response to subsequently verified authentication of the addressee:

transmitting the package to the addressee via the network.

2. (Original) The method of claim 1, wherein the step of determining whether the addressee has a public key comprises the sub-step of:

checking a public key directory for a public key of the addressee.

3. (Original) The method of claim 1, further comprising the step of:

storing the addressee's new public key in a public key directory.

3 of 11